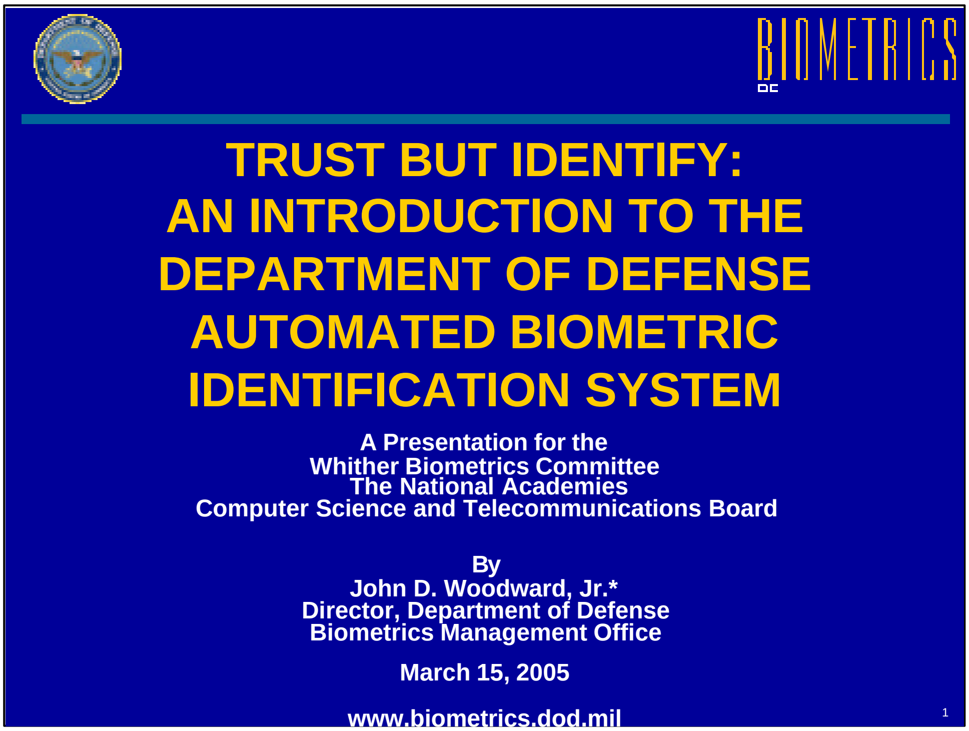


TRUST BUT IDENTIFY: AN INTRODUCTION TO THE DEPARTMENT OF DEFENSE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM

A Presentation for the
Whither Biometrics Committee
The National Academies
Computer Science and Telecommunications Board

By
John D. Woodward, Jr.*
Director, Department of Defense
Biometrics Management Office

March 15, 2005

www.biometrics.dod.mil

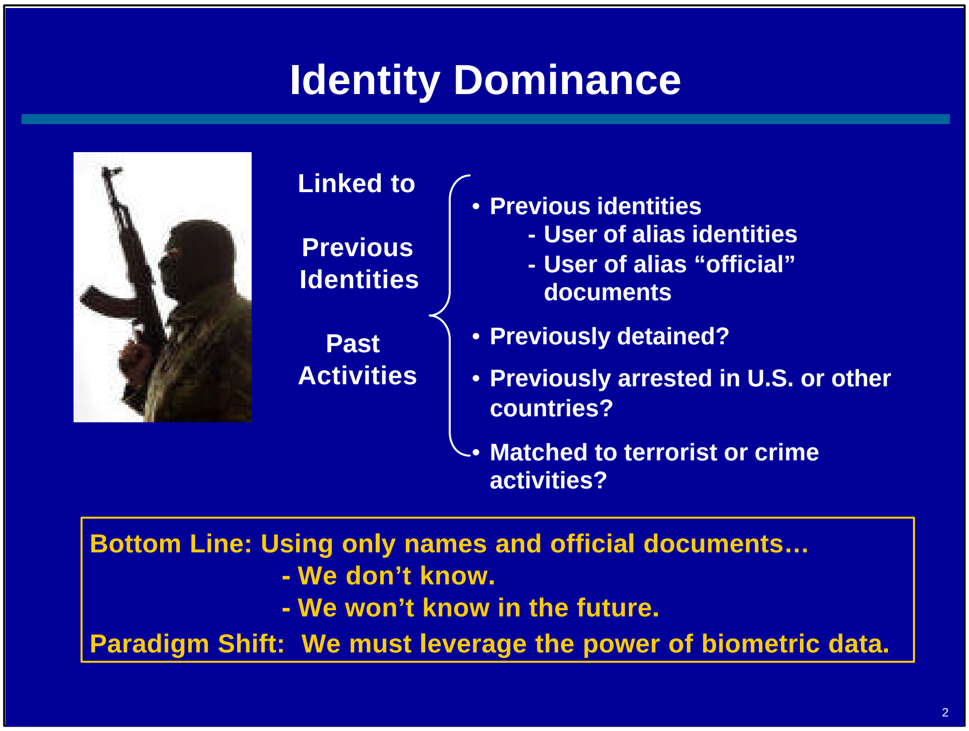
1

One of the good things about the Department of Defense Automated Biometric Identification System is that it makes for a very good acronym - "ABIS." Those of you familiar with law enforcement work might find this acronym familiar, as it takes its inspiration from the Federal Bureau of Investigation's Integrated Automated Fingerprint Identification System, inaugurated in 1999. The "IAFIS" contains, in a searchable, electronic format, the fingerprints of approximately 48 million people who have been arrested in the U.S. on felony or serious misdemeanor charges. The IAFIS is a true biometric workhorse that regularly identifies individuals with criminal histories, despite these individuals' best efforts to deny their criminal past.

In this briefing, I will highlight what we, in Department of Defense Biometrics, are currently doing with respect to using biometric capabilities in support of U.S. efforts in the Global War on Terrorism. By way of background, in August 2004, DoD leadership authorized a biometric identification system as a pilot effort, thus, the ABIS was born. The Department of Defense Biometrics Management Office, working with other DoD organizations, established this system shortly thereafter. In November 2004, DoD Biometrics Fusion Center formally became the central coordination point for detainee biometric data, the operational and technical element of my office.

Conceptually, the ABIS embodies what I call establishing "Identity Dominance." Operationally, the ABIS provides this critical support by storing, searching, and matching biometric data. More specifically, the ABIS stores, searches, and matches fingerprint data of non-U.S. persons that the U.S. military collects from detainees, enemy combatants, and other persons of interest.

* John D. Woodward, Jr., is the Director of the U.S. Department of Defense Biometrics Management Office. Mr. Woodward comes to the Department of Defense from RAND Corporation. He is the primary author of *Biometrics: Identity Assurance in the Information Age* (McGraw-Hill, 2003). The views and conclusions expressed in this annotated briefing are those of Mr. Woodward and do not necessarily represent those of the Department of Defense, any of its components, the RAND Corporation, or any of its research sponsors.



Identity Dominance

Linked to

Previous Identities

Past Activities

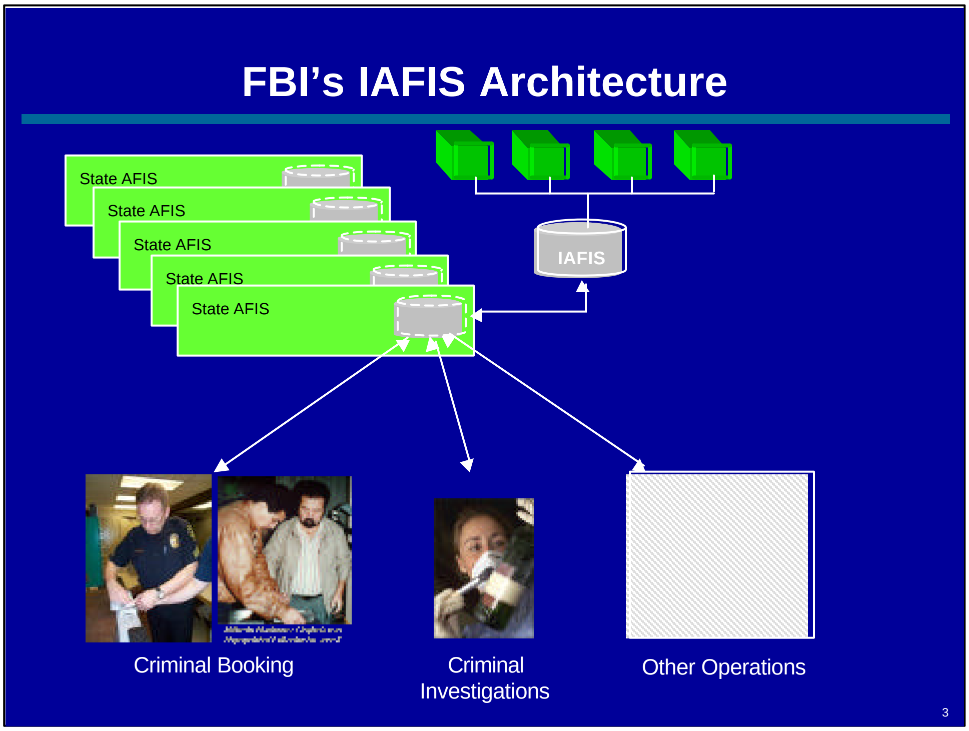
- Previous identities
  - User of alias identities
  - User of alias "official" documents
- Previously detained?
- Previously arrested in U.S. or other countries?
- Matched to terrorist or crime activities?

Bottom Line: Using only names and official documents…
- We don't know.
- We won't know in the future.
Paradigm Shift: We must leverage the power of biometric data.

Let's first discuss the concept: Identity dominance refers to the military's ability to link a person that the military has in custody as an enemy combatant, detainee, or similar person of interest to that person's previously used identities, or previous participation in terrorist or criminal activities. You can understand why identity dominance is important to the military, especially in view of current responsibilities in places like Iraq and Afghanistan. You can recognize that if we look at the Global War on Terrorism and focus on the adjective "global," we face an enemy that is very mobile and very motivated, and a foe that does not wear a traditional uniform or march under regimental colors. Rather, our enemy dons mufti and can skillfully go anywhere around the world to further activities that are extremely harmful to our nation and the American people. Through the Automated Biometric Identification System, we provide a powerful tool for identity dominance - enabling the military to positively identify enemy combatants on the battlefield using biometric data, and to establish links to a person's previously used identities and past criminal or terrorist acts.

The military encounters an individual on a foreign field, and wants to link that individual to previous identities and past activities. For example: Has the person been previously detained by the military? Has he or she been arrested in the U.S. or other countries? Have the individual's biometric data been matched to terrorists or crime scenes? Has the individual used previous identities? To the extent we try to do this based on names the person gives us, or based on so-called "official documents" the person carries, we will never get good answers.

I had the opportunity to speak at a recent military conference, and I made the argument that in my opinion, the best information the military can get from detainees is biometric information. I half-jokingly told the audience not to worry so much about names. Half the time they will lie about their names anyway. The other half of the time we cannot properly translate their foreign names into English script. Get the biometric information, because if you collect it correctly, you will have it forever, and it is very hard to change or alter biometric data, such as fingerprints. Perhaps I am being too biometric-centric; however, I firmly believe that using biometric data is essential to national security.



FBI's IAFIS Architecture

State AFIS

State AFIS

State AFIS

State AFIS

State AFIS

IAFIS

Criminal Booking

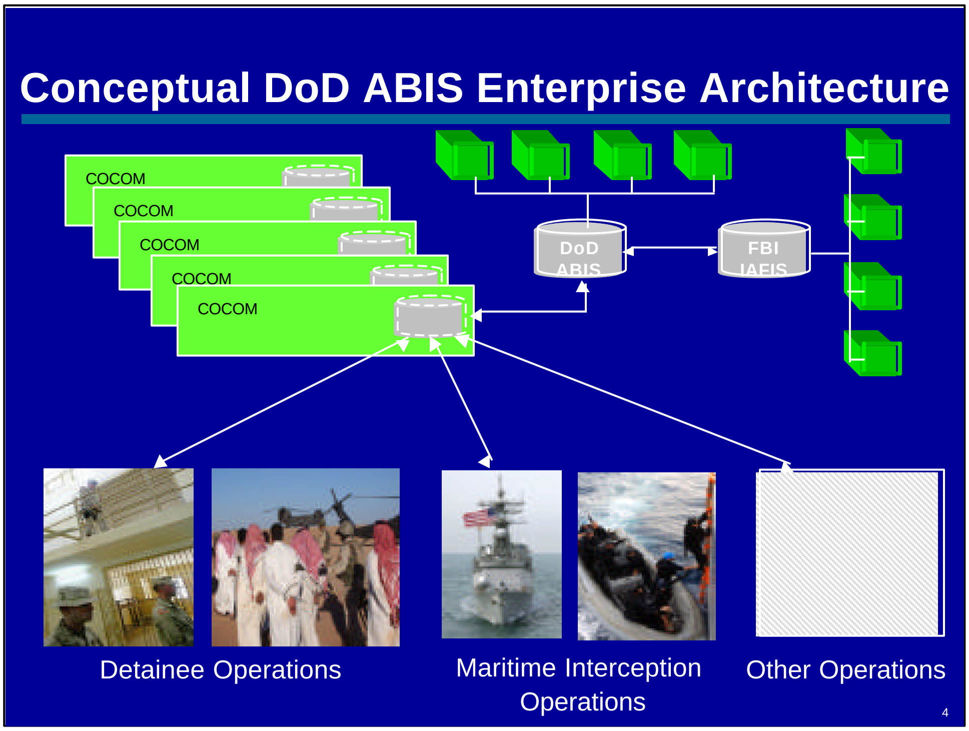
Criminal Investigations

Other Operations

3

Next, let's discuss the operational model of the ABIS. The slide above depicts a high-level overview of how the FBI's IAFIS system works. The ABIS is modeled on the IAFIS. We resisted the DoD tendency to "reinvent the wheel." IAFIS is a perfectly good wheel, and we modeled our ABIS efforts accordingly. Let's go through a criminal arrest, shown on the lower left-hand portion of the slide, as an example. Law enforcement does biometric collection during the booking process. Specifically, the police take mug shots. They also collect ten-rolled nail-to-nail fingerprints, using either (1) paper-and-ink cards and then electronically scan them into digital format, or (2) a fingerprint collection technology called "live scan," that uses computer processes and sensors to get the fingerprints electronically. One of the characteristics of fingerprints is that a person frequently leaves them behind, in the form of 'latents." In a law enforcement context, fingerprints are recovered from crime scenes. The latent fingerprints can be compared to fingerprint data and matched, as depicted in the lower middle portion of the slide.

Let me walk you through a generalized scenario. I get arrested in Criglersville, Virginia, and the police put me through the booking process and take my fingerprints. Those fingerprints are sent up to the state police in Virginia, where they have an automated fingerprint identification system, or "AFIS." From there, the fingerprints are sent to the FBI IAFIS and searched. The law enforcement community has a very strong interest in whether an individual has a previous criminal record. How fast is the search completed? The FBI receives approximately 25,000 criminal fingerprint submissions per day; 95% of those are searched and matched in less than two hours. The IAFIS is an extremely helpful tool--we quickly know whether the individual is a recidivist. The FBI's IAFIS makes it very difficult for someone with a criminal record to successfully say, "Officer, it's a terrible mistake. I've never been in trouble with the law before."



Conceptual DoD ABIS Enterprise Architecture

Detainee Operations

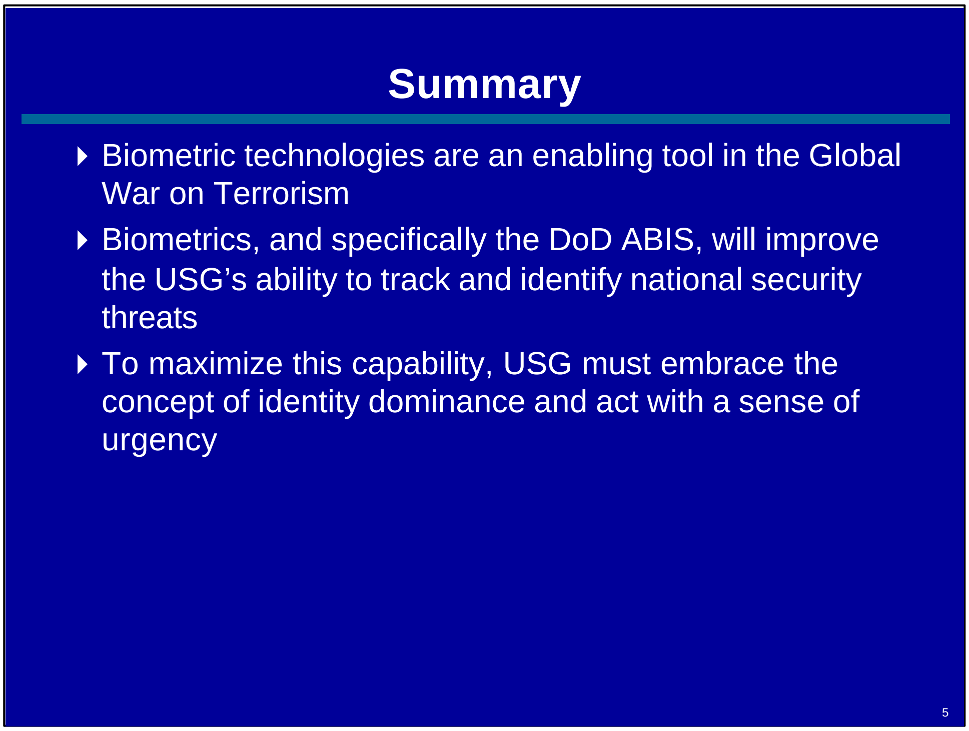
Maritime Interception Operations

Other Operations

At this point, the slide above showing the Department of Defense Automated Biometric Identification System should look familiar to you because as explained previously, we used IAFIS as our operational model. The slide above depicts a simplified conceptual architecture. Most of our current focus is on detainee and related operations, but we are working very hard to give the Navy a capability to use biometric data when they intercept ships on the high seas. When the military collects biometric data, it will be fed back to the Combatant Command. The war in Iraq is currently being fought in U.S. Central Command. The biometric data that the military collects from detainees is then transmitted to the DoD ABIS. The DoD Biometrics Fusion Center also shares that data with the FBI, where it is searched against the IAFIS database at the FBI's Criminal Justice Information Services Division, to see if the individual has an arrest record in the U.S., or is in the FBI known or suspected terrorist fingerprint database, which is also housed in the IAFIS. To be clear, the DoD's ABIS is fully interoperable with the FBI's IAFIS.

In 2005, the road-ahead for the DoD ABIS is connecting to organizations that will want to search against the databases, *i.e.*, fill-in the blank green boxes shown above. The ABIS is a new system, and it is not seamless and it is not perfect. There is a lot of baling wire and duct tape that holds it together for now.

Although many details cannot be publicly shared because of national security concerns, the ABIS, in its approximately seven months of operation, is making a difference. We have successfully used biometric data to identify individuals in military custody in Iraq as former detainees, as persons having U.S. criminal records, and as dangerous threats to U.S. forces.



Summary

- Biometric technologies are an enabling tool in the Global War on Terrorism
- Biometrics, and specifically the DoD ABIS, will improve the USG's ability to track and identify national security threats
- To maximize this capability, USG must embrace the concept of identity dominance and act with a sense of urgency

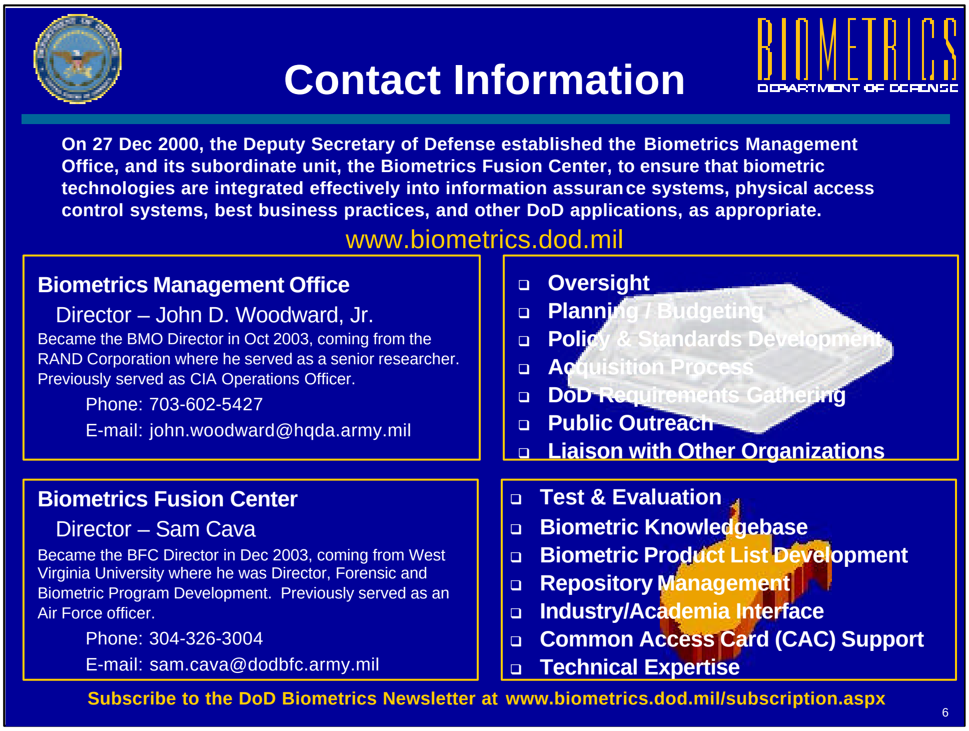
5

The military has always faced the challenge of identifying friend from foe. The Global War on Terrorism makes this challenge more difficult. While there is admittedly no silver bullet, biometrics are a very powerful weapon to link a person to previous identities and past activities. The Automated Biometric Identification System is protecting U.S. forces and protecting the nation - match by match.

A major challenge for DoD Biometrics in 2005 and 2006 is to improve and expand the ABIS capability out to more military units. We need to ensure that the military collects biometric data to the correct standard, and that the data gets transmitted to the ABIS in a timely manner for rapid searching, intelligence linking, and reporting of results.

Similarly, we must enable greater information sharing of our biometric data throughout the government, which includes our state and local partners. The goal of information sharing is to allow other government organizations to submit searches against the ABIS, to provide homeland security benefits. DoD Biometrics currently has several such information sharing initiatives under way.

In the near term, the ABIS will grow into a more robust and comprehensive system to help the military identify friend from foe.



BIOMETRICS
DEPARTMENT OF DEFENSE

Contact Information

On 27 Dec 2000, the Deputy Secretary of Defense established the Biometrics Management Office, and its subordinate unit, the Biometrics Fusion Center, to ensure that biometric technologies are integrated effectively into information assurance systems, physical access control systems, best business practices, and other DoD applications, as appropriate.

www.biometrics.dod.mil

Biometrics Management Office

Director – John D. Woodward, Jr.

Became the BMO Director in Oct 2003, coming from the RAND Corporation where he served as a senior researcher. Previously served as CIA Operations Officer.

Phone: 703-602-5427

E-mail: john.woodward@hqda.army.mil

- □ Oversight
- □ Planning / Budgeting
- □ Policy & Standards Development
- □ Acquisition Process
- □ DoD Requirements Gathering
- □ Public Outreach
- □ Liaison with Other Organizations

Biometrics Fusion Center

Director – Sam Cava

Became the BFC Director in Dec 2003, coming from West Virginia University where he was Director, Forensic and Biometric Program Development. Previously served as an Air Force officer.

Phone: 304-326-3004

E-mail: sam.cava@dodbfc.army.mil

- □ Test & Evaluation
- □ Biometric Knowledgebase
- □ Biometric Product List Development
- □ Repository Management
- □ Industry/Academia Interface
- □ Common Access Card (CAC) Support
- □ Technical Expertise

Subscribe to the DoD Biometrics Newsletter at www.biometrics.dod.mil/subscription.aspx

6

Selected Bibliography

Publications:

Beavan, Colin. *Fingerprints: The Origins of Crime Detection and the Murder Case That Launched Forensic Science*. New York: Hyperion (2001).

Cole, Simon A. *Suspect Identities: A History of Fingerprinting and Criminal Identification.* Cambridge: Harvard University Press (2001).

German, Ed. *Latent Fingerprint Examination: Fingerprints, Palm Prints, and Footprints.* Available at http://onin.com/fp/.

Jain, Bolle, and Pankanti. *Biometrics: Personal Identification in Networked Society.* Boston: Kluwer Academic Publishers (1999).

Wayman, Jain, Maltoni, and Maio. *Biometric Systems: Technology, Design and Performance Evaluation.* London: Springer (2005).

Woodward, Higgins, and Orlans. *Biometrics: Identity Assurance in the Information Age*. New York: McGraw-Hill/Osborne (2003).

Websites:

Department of Defense Biometrics

http://www.biometrics.dod.mil/

Federal Bureau of Investigation Criminal Justice Information Services Division

http://www.fbi.gov/hq/cjisd/cjis.htm